

September 11, 2014

Attention:

Cyber Crime Working Group Member - Honorable Brian Moran
Cyber Crime Working Group Member – J.C. Dodson
Cyber Crime Working Group Member - John Wood
Cyber Crime Working Group Chair - Paul Tiao

Department of State Police: Cyber Resource Critical Needs

Enforcement of the Commonwealth's criminal laws requires a level of expertise and an ability to sustain such expertise over the long-term. With the continued evolution of technology, such expertise is in extraordinary demand across the law enforcement community. This demand not only reflects increased complexity in the cyber threat environment, but it demonstrates that technology is an ever increasing facilitator of nearly all criminal activity.

The Virginia State Police supports the Commonwealth's 340 law enforcement agencies. Considerable technology gaps exist across the law enforcement community that the department strives to address. The agency takes this role seriously and has committed scarce resources to support federal, state, and local law enforcement investigations.

The unprecedented growth in the use of computers, mobile devices, and the Internet causes an emergence of computer crime and computer facilitated crime. This dynamic results in a growing demand on limited resources and a significant increase in the volume of digital media to be examined. The department faces increasing incidences of computer crime, including threats, child pornography, fraud, gambling, extortion, and identity theft. The department must also contend with the increase in criminal activity targeting computer networks, including hacking, malicious attacks, and denial of service. The investigation of computer crime is complex, requires extensive training and financial resources to sustain such capabilities.

The department's ability to successfully address this demand is adversely impacted by personnel shortages. The most recent Manpower Augmentation Plan identified staffing needs according to documented workload in each service area. As such, the subsequent paragraphs identify the "immediate" need. As this critical need for human resources is considered, it is imperative that education, equipment, and sustainability costs are included.

- **2 Digital Evidence Examiner Positions (Chesapeake and Wytheville)** – The Computer Evidence Recovery Section (CERS) Richmond Facility is currently staffed with four civilian examiners, one sworn examiner, one evidence technician, and a supervisor. The Northern Virginia Internet Crimes Against Children (ICAC) Lab is grant funded and staffed with one civilian examiner and

one part-time sworn examiner. It is anticipated that grant funding will permit the department to transition this part-time position to a full-time position in 2015. The newly established Roanoke lab is staffed with one civilian examiner, a position that was established by relocating a vacant Richmond position to serve the entire western and southern regions of the Commonwealth. The current case work reflects that approximately 35% of cases originate from this region, which does not include media that is inadvertently diverted to other agencies due to existing backlogs. Further, the Chesapeake region is home to an exploding population with no digital forensic support. This approximation substantiates the need to enhance this capacity to address the workload.

As with any service/support oriented effort, our ability to respond and address service respective requests is directly related to our level of future need and usefulness. Agencies and personnel not receiving the desired service will obviously pursue alternatives. These alternatives vary in quality and may not provide sound evidence collection practices. As such, our failure to actively address this issue will enhance the gaps in digital evidence collection/extraction to further deteriorate service to the region. Therefore, it is vital to add an examiner to Wytheville and Chesapeake to address this immediate gap in service. Future needs demand examiner positions in Culpeper and Appomattox.

- **2 Civilian Analyst Positions (Richmond)** – As the department is the primary agency for installing and operating Dialed Number Recorders (DNR) and the only state agency responsible for wire intercepts, it is imperative that appropriate support personnel be established to provide the data and analytical support for criminal investigators, as well as other local, state and federal law enforcement agencies. Collecting, analyzing, and documenting the volumes of data prevent the investigating agent from directing his/her attention to the criminal casework. This lack of analytical support causes this vital service to go largely unused, and potentially results in many investigative leads being undetected. Further, these analyst positions will enhance intelligence products in support of criminal investigations and the Virginia Fusion Center. Past efforts to have Fusion Center analysts address this analytical need have failed, because of the myriad of duties thrust upon the analyst sitting in the center. The evolution of technology demands analytical support to eliminate stove-piped environments and provide the critical links across the criminal enterprise that leads to successful law enforcement investigations.
- **7 Agents to Combat Cyber and Cyber-Facilitated Criminal Activity, and Field Triage of Digital Media** – In the late 1990's, the department created a single high-tech crimes agent in each of the seven field divisions due to an ever increasing need for technical expertise when conducting certain types of criminal investigations. At that time, the average family may have had simplistic cell phones and a home computer. In today's technology driven society, the average family has multiple laptops, desktops, storage devices, online gaming, iPods, tablets, e-readers, and almost everyone has a smart phone, not to mention the

advent of social media that has ever changed our society and opened new avenues for criminal deviance never previously imagined. As a result, not just “certain types” of cases involve technology, but almost every criminal investigation has a technological component. However, there still remains only a single investigator in each of the BCI Field Offices (7 investigators for the entire Commonwealth of Virginia) to address the proliferation of criminal activity that involves and/or utilizes technology. Not only do these agents support department criminal investigations, they also support local law enforcement in an effort to fill the gaps across the law enforcement community.

Furthermore, since the inception of the High Tech Crimes Division (HTCD) in 2009; the department has experienced a dramatic increase in the number of Internet related child exploitation cases requiring an agency response. While the official Northern Virginia/District of Columbia (NOVA/DC) ICAC region is defined to the northern half of Virginia (Culpeper and Fairfax Divisions) and the District of Columbia, our task force personnel routinely engage in cases that extend beyond these imaginary borders. As the statewide law enforcement agency, we are obligated to address and support others in this increasing crime trend and be at the forefront of protecting Virginia’s children. Existing investigating agents are inundated with computer crime investigations and digital triage requests. In the past 12 months, just five high tech crime agents have triaged in excess of 52 terabytes (52,000 GB) of digital media; thereby, preventing the media from being sent to our already overwhelmed laboratories, who examined 119 terabytes in 2013. While this is extremely beneficial to the CERS and the requesting investigator, this work is complex and time consuming. By further diverting these few human resources, we cause our overall high-technology efforts to deteriorate as employees become increasingly overwhelmed. Considering our investments to date and our statewide jurisdiction, the department is in the best position to handle this critical need to investigate cyber and cyber facilitated crimes, to include child exploitation crimes and on-scene digital triage. The HTCD has proven that critical digital evidence gathered on-scene during several high-profile investigations has led to swift arrests of dangerous individuals in our society.

Additionally, the department has seen the demand for high-technology services increase to the point where the law enforcement community realizes that digital evidence is part of nearly every crime. As such, they turn to the HTC Agents to extract digital evidence from a myriad of devices, while we simultaneously seek training and expect these agents to manage the growing computer-related case work. Virtually every investigation handled by law enforcement produces a mobile device that needs to be analyzed, and/or a computer/digital device that needs to be previewed/examined. Furthermore, time is of the essence and the case agent not only needs to immediately preserve digital evidence, but also retrieve the information promptly. This dynamic creates a demand for rapid response by overburdened and scarce resources.

Relying on our federal partners to fill this growing void is not reasonable, nor is it acceptable, as they too have limited resources that must be directed largely towards national and international cyber crime. This dynamic leaves many domestic cyber crimes largely unaddressed or at least given an extremely low priority. Furthermore, the vast majority of cyber criminal activity is at the local and state level. These crimes impact the Commonwealth's citizens daily and demand our swift attention.

This complex work requires constant training and practical skill application to remain proficient. To best address this complex and evolving dynamic, the department's "immediate" need is for additional HTC Agents to be assigned to the BCI Field Offices. These resources will serve to address the demands from the citizens of the Commonwealth, as well as the law enforcement community as a whole.

- **1 Surveillance Agent for the Technical Support Section (TSS) in Richmond**
– In 1990, the Technical Support Section was staffed with nine agents. Over the past 23 years, technology has continued to evolve and numerous new technologies have been added; however, the overall section staffing remains unchanged. In 2009, one of the Richmond positions was moved to Appomattox to provide coverage to a region that previously did not have technical support. As such, Richmond resources were reduced by one position.

This technical service is vital to the entire law enforcement community and is directly related to the success of numerous high profile criminal investigations. The vast majority of this technical equipment is housed and operated from Richmond, and it requires dedicated human resources to maintain and respond. Further, the personnel handling these duties are also responding to a wide array of technical support requests, which has caused the technology to exceed the capacity of the existing staff. In addition to day-to-day requests and support of investigations across the Commonwealth, personnel must engage in continuing education/training to support the additional technologies. Overall work for this section is 30% greater than the same quarter last year.

As articulated throughout this document, the identified human resources are essential to merely fill existing gaps and do not address long-term needs of this evolving environment. Furthermore, human resources are only one element of the gap analysis, as these resources require equipment, training, and sustainability in order to be effective. As such, approximate fiscal responsibilities are as follows:

Personnel (12)	\$1,200,000
Training/Equipment (Start-up)	\$400,000
Annual Sustainability (Trng. & Equip.)	<u>\$250,000</u>
Total	~\$1,850,000

Technology continues to evolve; communications are instantaneous and inexpensive. Although this high-speed world is convenient, it is, and will continue to be, exploited by criminal opportunists. As our society continues to rapidly consume information, we must not wait, we must act to fill the gaps. Addressing these gaps not only improves protection for our citizens, but it promotes economic growth across the Commonwealth, as corporate confidence encourages expansion and development. This endeavor is a true leadership opportunity.